BROCADE

Software Release 12.2.1b for Brocade ServerIron ADX Series Application Delivery Controllers

Release Notes v1.0

December 1, 2010

Document History

Document Title	Summary of Changes	Publication Date
Software Release v12.2.1b for Brocade ServerIron ADX Application Switches Release Notes v1.0	Initial release	December 1, 2010

Copyright © 2010 Brocade Communications Systems, Inc. All Rights Reserved.
Brocade, the B-wing symbol, ServerIron ADX, BigIron, DCX, Fabric OS, FastIron, IronPoint, IronShield, IronView, IronWare, JetCore, NetIron, SecureIron, ServerIron, ServerIron ADX, StorageX, and TurboIron are registered trademarks, and DCFM, Extraordinary Networks, and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: The information in this document is provided "AS IS," without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd*.

Export of technical data contained in this document may require an export license from the United States Government.

Contents

Supported Devices for Brocade ServerIron ADX 12.2.1 4
About This Release 4
Summary of Enhancements in ServerIron ADX 12.2.1 4
New Features of this Release (12.2.1) 4
Brocade ServerIron ADX ASM4 Bundle 4
IPv6 VIP Route Health Injection (RHI) 4
Lifting Subnet Mask Restriction for VIP RHI 5
Passive FTP support for Transparent Cache Switching Designs 5
Cache Server Persistence based on Custom String 5
Multi-Zone Firewall Load Balancing 5
Weighted Round Robin Static – A New Load Balancing Predictor 5
Auto Enable / Disable SYN Proxy Attack Protection 6
Deterministic Gateway Selection in Policy Based Routing (PBR) Configurations 6
Seamless handling of new Organization Unique Identifier (OUI) 6
Brocade IronView Network Manager / Device Management related Enhancements 6
Optimizing application delivery in IP NAT environment 6
Brief Summary of Software Features 7
Required Software Images 8
Image Files for ServerIron ADX 12.2.1b 8
Embedded Boot Images 9
Qualified USB Drives with the Release 9
Factory Pre-loaded Software 9
Supporting Documentation for ServerIron ADX release 12.2.1 10
Upgrading from release 12.1.0x to 12.2.0 or later 11
Upgrading a single management module from release 12.1.0x to 12.2.0 or later 11
Upgrading dual management modules from release 12.1.0x to 12.2.0 or later 12
Upgrading from 12.0.0 to 12.2.0 or later 13
Upgrading a single management module via an interface module port 13
Upgrade dual Management Modules via an interface module port 14
Technical Support 16
Closed with code in ServerIron ADX 12.2.1b 17
Closed with code in ServerIron ADX 12.2.1 26
Open Defects in the ServerIron ADX 12.2.1 38

Supported Devices for Brocade ServerIron ADX 12.2.1

This software release applies to the following Brocade ServerIron ADX controllers:

- Brocade ServerIron ADX 1000
- Brocade ServerIron ADX 4000
- Brocade ServerIron ADX 8000
- Brocade ServerIron ADX 10000

About This Release

This release supports a Layer 2 software image and a Layer 3 Software Image.

Summary of Enhancements in ServerIron ADX 12.2.1

The section describes the feature highlights in this release. Features or options not listed in this section or documented in the *Brocade ServerIron ADX Configuration Guides* are not supported.

New Features of this Release (12.2.1)

This section describes all of the new features that have been added with release 12.2.1.

Brocade ServerIron ADX ASM4 Bundle

Brocade is pleased to announce general availability of a new ASM4-based ADX 4000 bundle. This bundle extends the ServerIron ADX 4000 family and offers a new entry-level, modular application delivery controller platform. The bundle is delivered pre-configured with:

- one ASM4 application switch module (a software-restricted flavor of ASM8 module)
- one management module
- one 12-port Gigabit Ethernet fiber line card
- eight Gigabit Ethernet copper SFP connectors
- two AC power supplies
- premium software.

The ASM4 module is enabled for four application cores, and is upgradeable to eight application cores through the capacity-on-demand feature of the ServerIron ADX. Using a simplified, software license-upgrade approach, you can double application throughput capacity of the ASM4 bundle from 9 Gbps to 17.5 Gbps. If you add a second ASM8 module, then the performance will increase to 35 Gbps. This ASM4 bundle must run the Brocade ServerIron ADX software release 12.2.1 or later.

IPv6 VIP Route Health Injection (RHI)

Brocade ServerIron ADX offers two approaches for achieving traffic distribution among multiple sites: Global Server Load Balancing (GSLB) and VIP Route Health Injection. Both methods provide traffic distribution and site failure protection. Unlike GSLB, VIP route health injection is independent of the DNS infrastructure. It relies on the underlying routing infrastructure to achieve load balancing. Starting with this release, Brocade ServerIron ADX is extending support for VIP route health injection to IPv6 application services. This allows injection of IPv6 VIP routes inside the OSPF version 3 routing process meant for carrying IPv6 routes. Consequently administrators can

now roll-out VIP route health injection based multi-site redundancy solutions for both IPv4 and IPv6 application services.

Lifting Subnet Mask Restriction for VIP RHI

Historically, the ServerIron ADX has required that the subnet mask of an injected VIP route (through the VIP route health injection feature) be greater than the subnet mask of the respective interface. As an example, if a VIP route belonged to a subnet configured on an interface with a mask value "/24", then the minimum allowed mask for the VIP route had to be "/25" or greater. If an administrator wants to advertise the entire "/24" subnet, they need to independently inject two "/25" subnets. With this release, Brocade has lifted this restriction and allows configurations to accept a mask "equal-to" or "greater-than" the corresponding interface mask.

Passive FTP support for Transparent Cache Switching Designs

The Brocade ServerIron ADX provides for optimal distribution of traffic among cache servers through its Transparent Cache Switching or Redirection feature. This feature improves the cache-hit ratio and saves WAN bandwidth cost. The commonly used File Transfer Protocol (FTP) can run in either of the two modes: active FTP or Passive FTP. Previously, ServerIron ADX only offered support for transparent cache switching with Active FTP. This release extends transparent cache switching support to Passive FTP.

Cache Server Persistence based on Custom String

In a transparent cache redirection solution, it is critical to provide cache server persistence to minimize content duplication, maximize cache-hit ratio and save WAN bandwidth.

Prior releases of Brocade ServerIron ADX offered cache persistence based on the following: IP address, requested URL path, requested URL host name and requested URL parameters. This release extends this list by offering persistence based on custom string within a requested hostname or URL. A common example where this feature can be helpful is with video streams that users download from the Internet. Because each of these video streams has a unique video-id, the cache hit ratio can be significantly improved by persisting on a unique video-id string that resides inside requested URL.

Multi-Zone Firewall Load Balancing

The Brocade ServerIron ADX offers a powerful load balancing solution for infrastructure devices such as firewalls. You can distribute traffic load among multiple low-end or high-end firewalls and achieve flow persistence using the Brocade ServerIron ADX devices, and thereby achieve maximum return on your investment.

Previously, the Brocade ServerIron ADX supported firewall load balancing for up to 3 zones: internal, external and DMZ zones. With this release, support is extended for up to 8 zones for larger deployments that involve firewall devices supporting more than 3 zones. The number of firewall paths has been raised from 32 to 64, while the maximum supported firewall count is kept at 16.

Weighted Round Robin Static – A New Load Balancing Predictor

Predictors or load balancing algorithms play an important role in achieving traffic distribution among application servers. Brocade ServerIron ADX supports a variety of predictors including: least connections, round-robin, enhanced weighted, dynamic weighted and response time. Many of these predictors are connection-based which means that the application servers are picked based on the current connection load situation. While this is ideal in most situations, some designs require different treatment for traffic distribution. To handle such designs, Brocade is offering a new weighted-round-robin-static predictor that is completely agnostic of current connection load.

Auto Enable / Disable SYN Proxy Attack Protection

Brocade ServerIron ADX offers one of the best solutions in the industry for protection against TCP SYN attacks. This functionality is disabled by default and can be enabled on a per-interface basis. This release offers additional intelligence to automatically switch attack protection on-or-off depending on thresholds that are pre- specified by the administrator. When the connection rate exceeds a specified “ON-threshold”, the SYN proxy mechanism is enabled automatically, and when the connection rate drops below a specified “OFF-threshold”, the SYN proxy mechanism is disabled. This helps minimize connection establishment latency associated with proxy connections when infrastructure isn't under attack.

Deterministic Gateway Selection in Policy Based Routing (PBR) Configurations

When Policy Based Routing (PBR) is enabled on Brocade ServerIron ADX application delivery controllers running other layer 4 through 7 features, the gateway or next-hop selection for response traffic is usually driven by PBR policy. This may not be desired in situations where you want the L4-7 feature to determine your next-hop. With this release, the ServerIron ADX software allows administrators to specify a lower preference for PBR policy and prefer a gateway determined by other L4-7 features such as port spoofing.

Seamless handling of new Organization Unique Identifier (OUI)

As suggested by its name, the “Organization Unique Identifiers” are unique per organization. Vendor organizations use this unique identifier to assign MAC addresses to devices they manufacture. Larger organizations may require multiple identifiers to meet their MAC address needs.

The Brocade ServerIron ADX devices frequently use the built-in device MAC address to derive a virtual MAC address for the IP address that is shared between peer high-availability (HA) units. If two hardware units provisioned in HA mode have a different OUI, there can be problems in the event of an HA failover. Note that hot-standby HA configurations are not affected by such mismatches; however designs that use symmetric active-standby or active-active HA configurations may observe some problems in the case of an OUI mismatch. Generally speaking, its less likely to experience this at the field level if both HA units are ordered and received at the same time. Regardless, in the unlikely event of such a mismatch, the ServerIron ADX software is built with the necessary intelligence to resolve this conflict without requiring user configuration.

Brocade IronView Network Manager / Device Management related Enhancements

The release adds new SNMP MIBs and TRAPs for tracking licenses on the Brocade ServerIron ADX systems. These TRAPs are generated when a license is added or removed or about to expire. In addition, this release adds a new master password setting to simplify management of SSL certificates and SSL keys.

Optimizing application delivery in IP NAT environment

The software release includes enhancements that help optimize application delivery in environments that involve IP NAT. No user configuration is necessary to achieve this optimization.

Brief Summary of Software Features

The following is a brief highlight of features available with Brocade ServerIron ADX:

- Server Load Balancing (SLB) :
  A variety of load balancing algorithms (predictors)
  Inline and Direct Server Return (DSR) modes
  Local and remote servers
  Primary and backup servers
  Sticky and concurrent connections
  Port tracking
  Port aliasing
  Stateless SLB
- Application Health Checks :
  L2/3 ARP & ICMP checks
  Layer 4 TCP/UDP health checks
  Layer 7 application health checks
  Port profiles
  Port policies
  Element health checks
  Boolean health checks
- Layer 7 Content Switching (CSW) for application data aware traffic distribution :
  CSW for http protocol
  CSW for non-http applications such as FIX protocol
- High Availability (HA) modes :
  Hot-Standby
  Symmetric active standby
  Symmetric-active –active
- Secure Socket Layer (SSL) offload
- IPv6 Server Load Balancing :
  IPv666 (IPv6 VIP to IPv6 Real) SLB
  IPv664 (IPv6 VIP to IPv4 Real) SLB
  Static routing and OSPFv3 support for IPv6
  VRRP-E and HA support for IPv6
  IPv6 management
- Global Server Load Balancing for multi-site redundancy
- Transparent Cache Switching (for traffic distribution among cache servers)

- Security :
  Hardware based Syn-attack (Syn-Proxy) and other DoS attack prevention
  Syn-Defence for DSR topologies
  Transaction and Connection Rate Limiting
  Management Traffic Attack Protection
  Service Port Attack Protection
  Access Control Lists (ACLs)
  IP NAT
  SPAM mitigation using PBSLB
- Management :
  Telnet, SSHv2, SNMP, Syslog
  Web user interface
  Brocade INM
- Switching & Routing :
  Static Routing
  RIP, OSPFv2, OSPFv3
  VRRP
  VRRP-E for IPv4 and IPv6
  Route-only
  Spanning Tree Protocol – STP and RSTP
  VLAN
  Trunks (LACP and Etherswitch/Etherserver trunks)
  Tagging
- SIP server load balancing (for VOIP deployments)
- Firewall load balancing

Required Software Images

The ServerIron ADX Series of applications delivery controllers are upgraded using a single software image. This image is downloaded to the ServerIron ADX switch as either a Primary or Secondary. The default booting image is the Primary while the ServerIron ADX switch can be configured to boot from the Secondary.

Image Files for ServerIron ADX 12.2.1b

The following Switch Software Image Files are available for ServerIron ADX 12.2.1b.

Device	Layer 2 (switch image)	Layer 3 (router image)	Boot Image File
ServerIron ADX Series: All models	ASM12201b.bin	ASR12201b.bin	Included inside system image

Note: Brocade recommends using the latest software versions to get the greatest benefit from the ServerIron Application Delivery Controller. Check Brocade's knowledge portal for latest versions available.

Embedded Boot Images

The Brocade ServerIron ADX Software comprises multiple image files that are bundled together to form a single image. In simplistic terms, you could say that it consists of two parts:

1. **The application image:** This is the software that controls most of the ServerIron ADX operation and features. It changes with every software release.
2. **The Embedded Boot image:** This image includes smaller images including: boot image, FPGA image, mbridge image,etc.. These individual images may or may not change with every release. The table below summarizes the changes to these images with every release.

ServerIron ADX Software Release	Embedded Boot Image	Embedded boot image change description
12.0.0	First Release (12.0.00)	
12.1.0	Updated (boot ver 12.1.00 Oct 29, 2009)	Code flash RevF support Boot upgrader {flash | tftp} {primary | secondary | tftp } support
12.1.0a	No Change (boot ver 12.1.00 Oct 29, 2009)	
12.1.0b	No Change (boot ver 12.1.00 Oct 29, 2009)	
12.1.0c	Updated (boot ver 12.1.00ba Feb 26, 2010)	Changed both MP and BP DIMM setting
12.1.0d	No Change (boot ver 12.1.00ba Feb 26, 2010)	
12.1.0e	Updated (boot ver 12.1.00a Jul 9, 2010)	CPU version 2.1 support and bug fixes
12.1.0f	No Change (boot ver 12.1.00a Jul 9, 2010)	
12.2.0	Boot ver 12.1.00ba Feb 26, 2010, same as 12.1.0c	
12.2.0a	Updated (boot ver 12.1.00a Jul 9, 2010)	
12.2.1	Boot ver 12.1.00a Jul 9, 2010, same as 12.2.0a	
12.2.1b	Boot ver 12.1.00a Jul 9, 2010, same as 12.2.0a	

Qualified USB Drives with the Release

The external USB sticks (drives) that use a SmartModular or Unigen chip are qualified for use with ServerIron ADX. The external USB hard drives are not supported with Brocade ServerIron ADX.

Factory Pre-loaded Software

ServerIron ADX Application switches are pre-loaded with a switch image on both primary and secondary flash.

- If you place an order for a ServerIron ADX bundled with a PREM license, then the PREM license is activated on the unit. The unit still ships with layer 2 switch code on both primary and secondary flash. If desired, upgrade the unit to layer 3 code by downloading the code from the Brocade knowledge portal.

Supporting Documentation for ServerIron ADX release 12.2.1

This release note includes a list of supported features in Brocade ServerIron ADX software release 12.2.1. For specific details of the features, and all other information required to operate the devices, refer to the following manuals:

- Brocade ServerIron ADX Server Load Balancing Guide
- Brocade ServerIron ADX Advanced Server Load Balancing Guide
- Brocade ServerIron ADX Global Server Load Balancing Guide
- Brocade ServerIron ADX Security Guide
- Brocade ServerIron ADX Administration Guide
- Brocade ServerIron ADX Switching and Routing Guide
- Brocade ServerIron ADX Firewall Load Balancing Guide
- Brocade ServerIron ADX Graphical User Interface Guide
- Brocade ServerIron ADX Hardware Installation Guide
- IronWare MIB Reference

The Knowledge Portal (KP) contains the latest versions of these guides. You can also report errors on the KP. To access KP, log in to my.Brocade.com, click the Product Documentation tab, then click on the link to the Knowledge Portal (KP).

Upgrading from release 12.1.0x to 12.2.0 or later

The following procedures describe how to upgrade from release 12.1.0x to 12.2.0 or later in either a single or dual management module configuration.

NOTE : You must access the ADX system via console port while performing this upgrade if one of the embedded images have changed between software version your are upgrading from and software version you are upgrading to. Please refer to Embedded Boot Images section to see if your upgrade involves updating of embedded image.

Upgrading a single management module from release 12.1.0x to 12.2.0 or later

1. Copy the correct Brocade ServerIron ADX software image to a TFTP server.
2. Use the **copy tftp flash** command to download the software image to the ServerIron ADX from the TFTP server.

   ```
   ServerIronADX# copy tftp flash 1.1.1.1 asm12201.bin primary
   ```

   In the example above the software image is downloaded to flash as “primary”. When the ServerIron ADX reloads, it will boot using the primary image. Optionally, you can download the image as secondary by executing the following command.

   ```
   ServerIronADX# copy tftp flash 1.1.1.1 asm12201.bin secondary
   ```

3. Reload the system.

   Note : If the image was copied as secondary in Step 2, execute the following commands prior to reloading the ServerIron ADX.

   ```
   ServerIronADX (config)# boot system flash secondary
   ServerIronADX# write memory
   ServerIronADX# reload
   ```

   After reboot, the version checker may flag a warning message indicating a boot code mismatch. In such an event, follow Step 4 to upgrade the boot code.

4. Message from version checker

   If, after reloading the system as described in Step 3, you receive an ALERT message from the version checker stating that the boot code is mismatched, enter the following command at the application prompt to upgrade the boot code:

   ```
   ServerIronADX# boot upgrader flash <primary | secondary>
   ```

   When the system boots up through upgrader, enter:

   ```
   MP-appl# upgrade all
   ```

   NOTE : Once the boot upgrader has been invoked, you must continue the upgrade through a connection to the console port or else you will not be able to see the system screen through a remote Telnet / SSH connection.

5. Once the upgrade is complete, reload the unit.

Upgrading dual management modules from release 12.1.0x to 12.2.0 or later

This procedure applies to a ServerIron ADX system with 2 management modules installed.

1. Copy the correct Brocade ServerIron ADX software image to a TFTP server.
2. At the active management module, copy the 12.2.01 images to primary and secondary.

   ```
   ServerIronADX# copy tftp flash 1.1.1.1 asm12201.bin primary
   ServerIronADX# copy tftp flash 1.1.1.1 asm12201.bin secondary
   ```

   Wait for the new images on the active management module to be synced over to the standby management module. The following message will be displayed when the management modules are synced:

   ```
   ServerIronADX# sync secondary image: file not same
   sync to standby:  secondary image ... done. …
   ```

   It may take several minutes for this message to display. Do not proceed to the next step until it does.
3. Reload both management modules and they will both come up with the new application image.

   One management module will be in **active** mode and the other will be in **standby** mode.

   After reboot, the version checker may flag a warning message indicating a boot code mismatch. In such an event, follow Steps 4 - 6 to upgrade the boot code.
4. Reload both management modules and interrupt the normal boot cycle (for both) by pressing '**b**' to enter the monitor mode.

   ```
   ServerIronADX# reload
   Are you sure? (enter 'y' or 'n'): y
   Running Config data has been changed.   Do you want to continue
   the reload without saving the running config? (enter 'y' or 'n'): y
   Halt and reboot

   ServerIron Boot Code Version 12.1.0
   Enter 'a' to stop at memory test
   Enter 'b' to stop at boot monitor
   ***** Interrupted by entering 'b' *****

   BOOT INFO: load monitor from boot flash, cksum = 60f8
   BOOT INFO: verify flash files.....................
   Monitor> TSEC 0: 100 BASE-TX
   BP GE 0 Link Up

   Monitor>
   ```

   Check that both management modules (MPs) are in monitor mode before proceding to the next step. Proceding before both MPs are in monitor mode will cause the upgrade process to fail and render the system unstable.
5. On one of the management modules, enter the following command at the monitor prompt to upgrade the boot code:

   ```
   monitor> boot upgrader flash <primary | secondary>
   ```

   When the system boots up through upgrader, enter:

   ```
   MP-appl# upgrade all
   ```

   NOTE : Once the boot upgrader has been invoked, you must continue the upgrade through a connection to the console port.

6. Repeat Step 5 at the monitor prompt of the second management module.
7. Reload both management modules and use the show version command to verify that they are running the correct image.

Upgrading from 12.0.0 to 12.2.0 or later

Your ServerIron ADX may be running boot code version 12.0.00 (dob12000). This requires a one-time upgrade to boot code version 12.1.00 (dob12100). When upgrading the boot image, make sure that there are no power failures. A power failure during the upgrade procedure can result in the corruption of the existing boot code and may require you to RMA the management module.

NOTE : You must access the ADX system via console port while performing this upgrade if one of the embedded images have changed between software version your are upgrading from and software version you are upgrading to. Please refer to Embedded Boot Images section to see if your upgrade involves updating of embedded image.

Upgrading a single management module via an interface module port

1. Make sure that both the primary and secondary flash images (currently installed) are version 12.0.00.

   These images can be of any 12.0.00 revison (a, b, c etc).

2. Check that the system is configured to boot from primary flash. To be sure, issue the following command and save the configuration.

   ```
   ServerIronADX# no boot system flash secondary
   ServerIronADX# write memory
   ```

3. Copy the **12.1.00 upgrader** image from a TFTP server to secondary flash, as shown.

   ```
   ServerIronADX# copy tftp flash 1.1.1.1 A1B12100.bin secondary
   ```

4. Boot the system from the secondary flash (that contains the upgrader image installed in Step 3).

   ```
   ServerIronADX# boot system flash secondary
   ```

   The **boot system flash secondary** command forces the system to reboot from secondary flash regardless of the setting in the startup-config file.

   The system reboots and enters the upgrade mode.

5. Enter the **upgrade all** command at the console.
6. Once the upgrade process is complete, use the **reload** command to boot the system.

   The system will boot-up from the primary image which still contains 12.0.00 code. The system image at this stage is 12.0.00 and the boot code is 12.1.00.

7. Execute the **show version** command to confirm that the boot code upgrade has occurred correctly.
8. Copy the **12.2.01 application** image to primary and secondary flash from a TFTP server, as shown.

   ```
   ServerIronADX# copy tftp flash 1.1.1.1 asm12201.bin primary
   ServerIronADX# copy tftp flash 1.1.1.1 asm12201.bin secondary
   ```

   This procedure overwrites the 12.0.00 image on primary flash and the upgrader image on the secondary flash.

9. Execute the **show flash** command to verify that the image files have been copied correctly.

   The display should appear as follows :

   ```
   ServerIronADX# show flash
   ```

```
Active management module:
Compressed Pri Code size = 23311360, Version 12.2.00B2T401 May 23 2010 11:20:26 PST label:
ASM12201
Compressed Sec Code size = 23311360, Version 12.2.00B2T401 May 23 2010 11:20:26 PST label:
ASM12201
...
```

If the **show flash** command display is as shown below, the secondary image is not the application image and you will need to copy an application image to the secondary.

```
ServerIronADX# show flash
Active management module:
Compressed Pri Code size = 23311360, Version 12.2.00B2T401 Feb 12 2010 11:20:26 PST label:mp
ASM12100B2
Compressed Pri Code size = 6823553, Version 12.1.00T401 Oct 29 2009 10:12:47 PST label:mp
```

10. Reboot the system from the either primary or secondary flash.

    After reboot, the version checker will flag a warning message indicating a boot code mismatch. Follow step 11 to upgrade the boot code.

11. Message from version checker

    After reloading the system as described in step #10, there is an ALERT message from the version checker, stating that the boot code is mismatched. Enter the following command at the application prompt to upgrade the boot code:

    ```
    ServerIronADX# boot upgrader flash <primary | secondary>
    ```

    When the system boots up through upgrader, enter:

    ```
    MP-appl# upgrade all
    ```

    Once the upgrade is complete reload the unit.

    NOTE : Once the boot upgrader has been invoked, you must continue the upgrade through a connection to the console port.

12. After a successful reboot, use the show version command to verify that the ServerIron ADX is running the correct image.

Upgrade dual Management Modules via an interface module port

This procedure applies to a ServerIron ADX with 2 management modules installed.

NOTE : You must access both systems via their management module console ports while performing this upgrade.

1. Make sure that both the primary and secondary flash images (currently installed) on both the active and standby management modules are version 12.0.00.

   These images can be of any 12.0.00 revison (a, b, c etc).

2. On the active managment module, copy the 12.1.00 upgrader image from a TFTP server to secondary flash, as shown.

```
ServerIronADX# copy tftp flash 1.1.1.1 A1B12100.bin secondary
.....................................................................
.....................................................................
.............................
TFTP to Flash Done.
 done.
```

3. The system now initiates synchronization of the new secondary image (i.e. A1B12100.bin) from the active management module to the second management module. .

   The following message will be displayed when the management modules are synced:

   ```
   ServerIronADX#sync secondary image: file not same

   sync to standby:  secondary image ... done.
   ```

   It may take several minutes for this message to display. Do not proceed to the next step until it does.

4. Reload both management modules and interrupt the normal boot cycle (for both) by pressing '**b**' to enter the monitor mode.

   ```
   ServerIronADX# reload
   Are you sure? (enter 'y' or 'n'): y
   Running Config data has been changed.   Do you want to continue
   the reload without saving the running config? (enter 'y' or 'n'): y
   Halt and reboot

   ServerIron Boot Code Version 12.0.0
   Enter 'a' to stop at memory test
   Enter 'b' to stop at boot monitor
   ***** Interrupted by entering 'b' *****

   BOOT INFO: load monitor from boot flash, cksum = 60f8
   BOOT INFO: verify flash files.....................
   Monitor> TSEC 0: 100 BASE-TX
   BP GE 0 Link Up

   Monitor>
   ```

   Check that both management modules (MPs) are in monitor mode before proceding to the next step. Proceding before both MPs are in monitor mode will cause the upgrade process to fail and render the system unstable.

5. Boot **one** of the management modules (it doesn't matter which) from the secondary flash (containing the upgrader image installed in Step 2).

   ```
   Monitor> boot system flash secondary
   ```

   The **boot system flash secondary** command forces the system to reboot from secondary flash regardless of the setting in the startup-config file.

   The system reboots and enters the upgrade mode.

6. Enter the **upgrade all** command at the console of the management module that was just rebooted..
7. Reload the management module and place it back into monitor mode as in Step 4.
8. Go to the console of the management module that hasn't been upgraded and perform the boot from the secondary flash and **upgrade all** as performed on the first management module is Step 5 and Step 6.
9. Reload both management modules from the primary image.

   Both management modules will come up with the existing 12.0.00 image from the primary. One of the management modules will be in **active** mode and the other will be in **standby** mode. The system image at this stage is 12.0.00 and the boot code is 12.1.00.

10. At the active management module, copy the 12.2.01 images to primary and secondary.

    ```
    ServerIronADX# copy tftp flash 1.1.1.1 asm12201.bin primary
    ServerIronADX# copy tftp flash 1.1.1.1 asm12201.bin secondary
    ```

Wait for the new images on the active management module to be synced over to the standby management module. The following message will be displayed when the management modules are synced:

```
ServerIronADX#sync secondary image: file not same
sync to standby:  secondary image ... done. …
```

It may take several minutes for this message to display. Do not proceed to the next step until it does.

11. Reload both management modules and they will both come up with the new application image.

    One managment module will be in **active** mode and the other will be in **standby** mode.

    After reboot, the version checker will flag a warning message indicating a boot code mismatch. Follow step 12 to upgrade the boot code.

12. After reboot, the version checker will flag a warning message indicating a boot code mismatch.
13. Reload both management modules and place them in monitor mode as described in Step 4.
14. On one of the management modules, enter the following command at the monitor prompt to upgrade the boot code:

    ```
    monitor> boot upgrader flash <primary | secondary>
    ```

    When the system boots up through upgrader, enter:

    ```
    MP-appl# upgrade all
    ```

    NOTE : Once the boot upgrader has been invoked, you must continue the upgrade through a connection to the console port.

15. Repeat Step 14 at the monitor prompt of the second management module.
16. Reload both management modules and use the show version command to verify that they are running the correct image.

Technical Support

Contact your switch supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information immediately available:

General Information

- Technical Support contract number, if applicable
- Switch model
- Switch operating system version
- Error numbers and messages received
- Detailed description of the problem, including the switch or network behavior immediately following the problem, and specific questions
- Description of any troubleshooting steps already performed and the results
- Switch Serial Number

Closed with code in ServerIron ADX 12.2.1b

Defect ID: DEFECT000301639	**Technical Severity:** High
Summary: TCS hashing needs to be synchronized between Application processors (BP) on a given System.	
Symptom: Although ServerIron ADX is configured with hash-mask of 255.255.255.255 0.0.0.0, traffic destined to same IP address from different client ip addresses and processed by differnt BPs, will be sent to different cache server causing persistency to break.	
Probability: High	
Feature: TCS	**Function:** TCS L4
Reported In Release: SI 12.1.00	**Service Request ID:** 250411

Defect ID: DEFECT000303104	**Technical Severity:** Medium
Summary: Layer 7 Health Check response in very small fragments causes a server port's health check to get stuck in the Testing state	
Symptom: L4 and L7 keepalives will stop functioning if the real servers are sending very small (2 - 20 bytes) responses to L7 keepalives.	
Workaround: If "server fast bringup" is configured, the problem is not observed as keepalive handles these small packets correctly.	
Probability: Low	
Feature: Health checks	**Function:** L7 health checks
Reported In Release: SI 12.1.00	**Service Request ID:** 246820

Defect ID: DEFECT000304720	**Technical Severity:** Medium
Summary: Management interface IP address should not be treated as one of the eligible candidates for the local site IP address on a ServerIron ADX configured as local GSLB site .	
Symptom: Management interface IP address should not be treated as one of the eligible candidates for the local site IP address on a ServerIron ADX configured as local GSLB site. If this ip address happens to be the lowest ip address amongst all configured ip address on a ServerIron ADX then local GSLB site will not come up.	
Workaround: Do not configure management IP as lowest the IP address on the GSLB controller if the controller is also used as site.	
Probability: High	
Feature: GSLB	**Function:** GSLB controller
Reported In Release: SI 12.1.00	**Service Request ID:** 254510

Defect ID: DEFECT000307655	**Technical Severity:** Medium
Summary: Applying Debug filter substantially raises the CPU utilization on management and application processors.	
Symptom: SLB service may not work properly and high-availability features may fail-over to the secondary unit.	
Workaround: Do not use debug filter.	
Probability: High	
Feature: Debug filter	**Function:** Debug filter : Software
Reported In Release: SI 12.1.00	**Service Request ID:** 254444

Defect ID: DEFECT000310603	**Technical Severity:** Medium
Summary: The "show server ip-load-balancing bind" command exists in the CLI, but the "ip-load-balancing" feature is not supported on this platform.	
Symptom: Under virtual server, configuring 'ip-load-balancing' under a virtual server does not work but 'show server ip-load-balancing bind' is available in the CLI.	
Workaround: IP-load-balancing is not supported and should not be configured.	
Probability: High	
Feature: IP load balancing	**Function:** IP load balancing
Reported In Release: SI 12.1.00	**Service Request ID:** 257487

Defect ID: DEFECT000315376	**Technical Severity:** Medium
Summary: Ignore packet counter on per port will not include count for intentionally dropped packets.	
Symptom: Ignore counters incrementing on trunk port when ARP broadcast packets are send from ADX1 to ADX2 over the trunk.	
Probability: High	
Feature: Port	**Function:** Show/Clear commands
Reported In Release: SI 12.1.00	**Service Request ID:** 258427

Defect ID: DEFECT000316597	**Technical Severity:** Medium
Summary: The command 'clear server traffic' does not clear the 'max TCP attack rate' counter.	
Symptom: The command 'clear server traffic' does not clear the 'max TCP attack rate' counter.	
Probability: High	
Feature: CLI	**Function:** Clear Commands
Reported In Release: SI 12.1.00	**Service Request ID:** 258857

Defect ID: DEFECT000317410	**Technical Severity:** High
Summary: The error log message "Max Conn Reached" is erroneously logged for Real Server under certain conditions.	
Symptom: A real server bound to a VIP may stop receiving load balanced traffic. The ServerIron ADX logs will show the following message for the problematic real server: "L4 server <server-ip> <server-name> max connections 2000000 reached" The output of the command "show server session" will show an usually high PeakConn value.	
Workaround: N/A	
Probability: Medium	
Feature: L4 Server Selection	**Function:** Least Connection
Reported In Release: SI 12.2.00	**Service Request ID:** 260720

Defect ID: DEFECT000317525	**Technical Severity:** Medium
Summary: ServerIron ADX fails to perform Policy Based Routing (PBR) for ACTIVE FTP data connection and drops the packets when a default gateway is not available.	
Symptom: ServerIron ADX is configured with PBR for reverse SLB traffic and default gateway is either not configured or unavailable. When real server tried to open ACTIVE FTP DATA connection, ServerIron ADX dropped the TCP SYN packet from the real server even though PBR rule matched and the nex-hop router in the policy was available.	
Probability: High	
Feature: Policy based routing	**Function:** Policy based routing : SLB
Reported In Release: SI 12.1.00	**Service Request ID:** 255665

Defect ID: DEFECT000320071	**Technical Severity:** High
Summary: Using snmpset to try to write the running config to NVRAM leaves the ADX in a state where the "reload" command no longer functions.	
Symptom: Using snmpset to try to write the running config to NVRAM leaves the ADX in a state where the "reload" command no longer functions. More specifically, using snmpset to set snAgWriteNVRAM to 3, the value required to save the running config to NVRAM, leaves the ADX in a state where every attempt to execute the "reload" command returns the error message "System is in the middle of Flash write operation, please try later." Every attempt to perform snmpwalk or snmpget against snAgWriteNVRAM afterwards results in a 4, the value for "agent is writing NVRAM flash".	
Probability: High	
Feature: SNMP Management	**Function:** System Management Mib
Reported In Release: SI 12.1.00	**Service Request ID:** 263085

Defect ID: DEFECT000320215	**Technical Severity:** Medium
Summary: ACLs do not work for link-local scope of multicast address 224.0.0.0/24.	
Symptom: For link-local multicast address 224.0.0.0/24 access-lists will not work.	
Probability: Medium	
Feature: ACL	**Function:** IPv4 ACL
Reported In Release: SI 12.1.00	**Service Request ID:** 262805

Defect ID: DEFECT000320373	**Technical Severity:** High
Summary: For 4 BP Serveriron ADX systems, traffic counters on the MP do not get updated under certain conditions.	
Symptom: The counters on the MP may not be shown as updated.	
Workaround: Reset the PAX using 'pax hw reset'.	
Probability: Low	
Feature: Counter Sync	**Function:** FPGA functionality
Reported In Release: SI 12.1.00	**Service Request ID:** 262174

Defect ID: DEFECT000320377	**Technical Severity:** High
Summary: Client Connection Limit with SSL Termination does not work.	
Symptom: When "client-connection-limit" is configured and assigned to a VIP with SSL Terminated traffic and is applied to an interface, ServerIron ADX starts dropping the requests.	
Probability: High	
Feature: Conn Limit	**Function:** TCP Max Conn
Reported In Release: SI 12.1.00	**Service Request ID:** 261683

Defect ID: DEFECT000320384	**Technical Severity:** High
Summary: In Client Connection Rate Limiting, current connection counter will increment if the real server is down.	
Symptom: When Client connection rate limiting is configured and if the real server is down, current connection counter will keep on incrementating. If the real server comes up, the current connection counter may have already reached max-conn and hence new connections will get rate limited unnecessarily.	
Workaround: Use “clear conn all” to reset the counter.	
Probability: High	
Feature: Conn Limit	**Function:** TCP Max Conn
Reported In Release: SI 12.1.00	**Service Request ID:** 256456

Defect ID: DEFECT000320389	**Technical Severity:** High
Summary: Health check status is not synchronized from MP to BPs under certain conditions causing SLB failure	
Symptom: Real servers status will show active on the MP but they could be in failed or testing state on BPs.	
Probability: Low	
Feature: Health checks	**Function:** L4 health checks
Reported In Release: SI 12.1.00	**Service Request ID:** 262174

Defect ID: DEFECT000320639	**Technical Severity:** High
Summary: The command "url debug" does not work when used with Client-IP on the BP console.	
Symptom: No output is seen after enabling "url debug" with a Client-IP specified. The connection works but no debug output is received.	
Workaround: Use "url debug" without specifying a Client-IP. CAUTION: This should only be done if the client requests are less than 10. CPU utilization may spike up to unacceptable levels if the command is used where there are a large number of connections.	
Probability: High	
Feature: L7 SLB Full Stack	**Function:** Debug
Reported In Release: SI 12.1.00	**Service Request ID:** 259561

Defect ID: DEFECT000321367	**Technical Severity:** High
Summary: GSLB Transparent Intercept Does Not Work on a ServerIron ADX.	
Symptom: GSLB transparent intercept does not work as expected. Queries for all domains (including those not configured on the ServerIron ADX) are intercepted by the GSLB controller.	
Probability: High	
Feature: GSLB	**Function:** GSLB controller
Reported In Release: SI 12.1.00	**Service Request ID:** 263431

Defect ID: DEFECT000321795	**Technical Severity:** Critical
Summary: A ServerIron ADX might perform a system reset when PBR is configured and applied on a global level.	
Symptom: A ServerIron ADX will perform reset when PBR is configured with ip policy applied globally.	
Workaround: Apply the ip policy locally on the interface.	
Probability: Medium	
Feature: Policy based routing	**Function:** IP Policy
Reported In Release: SI 12.1.00	**Service Request ID:** 264523

Defect ID: DEFECT000321884	**Technical Severity:** High
Summary: A ServerIron ADX Application Processor may get reset upon receiving fragmented UDP packets when GSLB is configured.	
Symptom: Application processor might get reset when GSLB is configured.	
Probability: Low	
Feature: GSLB	**Function:** GSLB affinity
Reported In Release: SI 12.1.00	**Service Request ID:** 263981

Defect ID: DEFECT000321922	**Technical Severity:** High
Summary: A ServerIron ADX may perform system reset while deleting a Real Server Port in Health-check-Track-Group.	
Symptom: A ServerIron ADX may perform system reset while deleting a Real Server Port in Health-check-Track-Group.	
Probability: High	
Feature: Health checks	**Function:** L4 health checks
Reported In Release: SI 12.1.00	**Service Request ID:** 261604

Defect ID: DEFECT000322029	**Technical Severity:** High
Summary: ServerIron ADX may perform a system reset upong receiving a malformed SIP packet ending with "0d xx", where xx represents any ASCII characters.	
Symptom: ServerIron ADX may perform a system reset upong receiving a malformed SIP packet ending with "0d xx", where xx represents any ASCII characters.	
Probability: High	
Feature: SIP LB	**Function:** SIP Transport Layer Management
Reported In Release: SI 12.2.00	**Service Request ID:** 262561

Defect ID: DEFECT000322088	**Technical Severity:** Medium
Summary: In L7 switching with TCS, a Serveriron ADX does not generate any Log messages when the max-conn value is reached for a cache-server.	
Probability: High	
Feature: TCS	**Function:** TCS + URL switching
Reported In Release: SI 12.1.00	**Service Request ID:** 261025

Defect ID: DEFECT000322208	**Technical Severity:** High
Summary: A ServerIron ADX configured for "SLB proxy TCS" may process pass-through traffic and send it to cache servers under certain circumstances	
Symptom: When a ServerIron ADX is configured for SLB proxy TCS and both port 80 and port 8080 are defined under the cache servers, pass-through traffic with destination port 8080 is sent to cache servers even if the policy is only defined for HTTP.	
Probability: High	
Feature: TCS	**Function:** TCS L4
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000322241	**Technical Severity:** Medium
Summary: SSL part # section in the "Show Version" command output displays random characters.	
Symptom: SSL part # section in the "Show Version" command output displays random characters.	
Probability: High	
Feature: Character I/O	**Function:** Character Handling
Reported In Release: SI 12.2.00	

Defect ID: DEFECT000322253	**Technical Severity:** Critical
Summary: A ServerIron ADX Management Module resets while performing FWLB health checks.	
Symptom: A ServerIron ADX Management Module resets while performing FWLB health checks.	
Workaround: N/A	
Probability: High	
Feature: Health checks	**Function:** L3 health checks
Reported In Release: SI 12.1.00	**Service Request ID:** 00264180

Defect ID: DEFECT000322255	**Technical Severity:** Critical
Summary: With a ServerIron ADX configured for FWLB, an application processor (BP) may perform a reset while updating firewall path information.	
Symptom: With a ServerIron ADX configured for FWLB, an application processor (BP) may perform a reset while updating firewall path information.	
Probability: High	
Feature: FWLB	**Function:** Health check/Path discovery
Reported In Release: SI 12.1.00	**Service Request ID:** 00264180

Defect ID: DEFECT000322926	**Technical Severity:** Medium
Summary: A ServerIron ADX completes the TCP handshake even when all the servers are down in SSL session-id switching.	
Symptom: A client connecting via SSL will see a TCP handshake go through but will get a reset when it sends an SSL hello.	
Probability: High	
Feature: L7 SLB Pseudo Stack	**Function:** TCP Control packet handling
Reported In Release: SI 12.1.00	**Service Request ID:** 262891

Defect ID: DEFECT000323338	**Technical Severity:** Critical
Summary: With ServerIron ADX configured for AAA with TACACS+, authentication and authorization requests may fail as it uses random source IP addresses while initiating TCP connection to TACACS+ server.	
Symptom: TCP connections to TACACS+ server for Authentication requests by ServerIron ADX are sent with a Random IP addresses.	
Probability: High	
Feature: AAA	**Function:** AAA Engine
Reported In Release: SI 12.1.00	**Service Request ID:** 263789

Defect ID: DEFECT000323645	**Technical Severity:** Medium
Summary: ServerIron ADX does not perform periodic health-checks for port 3389. After the initial bringup, ADX stop sending continuous checks for L4 port status.	
Symptom: Period health-checks are not performed for port 3389.	
Workaround: Configure healthcheck-policy for port 3389 and identify the protocol as HTTP.	
Probability: High	
Feature: Health checks	**Function:** L4 health checks
Reported In Release: SI 12.1.00	**Service Request ID:** 265698

Defect ID: DEFECT000324567	**Technical Severity:** Medium
Summary: The command "write mem" does not get executed on ServerIron ADX and it throws an error "ERR: open write file" under certain conditions.	
Symptom: The command "write mem" does not get executed on ServerIron ADX and it throws an error "ERR: open write file" under certain conditions. Once this error is seen then all consecutive "write mem" commands do not get executed.	
Probability: Low	
Feature: MP System	**Function:** CLI
Reported In Release: SI 12.2.01	**Service Request ID:** 00266532

Defect ID: DEFECT000325261	**Technical Severity:** Critical
Summary: Transaction Rate Limiting (TRL) for UDP does not work if the command "ip udp trans-rate threshold " is configured globally.	
Symptom: Transaction Rate Limiting (TRL) for UDP does not work if the command "ip udp trans-rate threshold " is configured globally.	
Workaround: In the lab, we found that after removing the global command, ip udp trans-rate threshold 100 UDP trl worked as desired.	
Probability: High	
Feature: TRL	**Function:** UDP Conn Rate
Reported In Release: SI 12.2.01	**Service Request ID:** 266431

Defect ID: DEFECT000325686	**Technical Severity:** High
Summary: With "slb-use-internal-tcam" configured, "route-only" command is effective for all interfaces of a line card even though it is defined on a single interface.	
Symptom: Route-only action gets applied to all the interfaces of the line card even though it is defined on a single interface.	
Workaround: Use external TCAM	
Probability: High	
Feature: Route-only	**Function:** Forwarding
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000326028	**Technical Severity:** Critical
Summary: A Qualys tool while performing test on a ServerIron ADX configured for SSL-terminated VIP may report a vulerability issue related to TCP ISN (Initial Sequence Number) such as CERT Advisory CA-2001-09.	
Symptom: A Qualys tool while performing test on a ServerIron ADX configured for SSL-terminated VIP may report a vulerability issue related to TCP ISN (Initial Sequence Number) such as CERT Advisory CA-2001-09.	
Probability: Low	
Feature: TCP stack	**Function:** Stack
Reported In Release: SI 12.1.00	**Service Request ID:** 266506

Defect ID: DEFECT000326039	**Technical Severity:** Critical
Summary: ServerIron ADX creates an invalid IP cache entry for Virtual Server IP with flags DW (action DROP and WAITING on ARP entry for next-hop) when MP directly receives TCP/UDP traffic, due to L4-7 policy lookup failure, destined to VIP for which it is ACTIVE.	
Symptom: ServerIron ADX creates an invalid IP cache entry for Virtual Server IP with flags DW (action DROP and WAITING on ARP entry for next-hop) when MP directly receives TCP/UDP traffic, due to L4-7 policy lookup failure, destined to VIP for which it is ACTIVE. This is seen only when the VIP traffic is received with destination MAC as VE or physical interface MAC address of ServerIron ADX instead of VIP MAC. Subsequent incoming packets will be dropped dropped by hardware if L4-7 policy lookup continues to fail. This will cause ignore packet count to increment.	
Probability: Low	
Feature: IP Forwarding	**Function:** HW L3 forwarding
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000326109	**Technical Severity:** Critical
Summary: With SNMP based cache SLB, ServerIron ADX may perform a system reset when removing and adding snmp-request oid under cache server.	
Symptom: In SNMP based Cache server load balancing all SNMP request OIDs are set under each cache server. When this configuration is removed from a cache server using the commands 'no snmp-request community .....' and 'no snmp-request oid 1 1.3…..' and then reapplied under the cache server, System may perform reset.	
Workaround: You can follow the following steps to re-add the SNMP configuration: 1) Remove the binding from under the Virtual Server for the cache server to which the MIB needs to be added. 2) Configure the SNMP community and the MIB under the cache server. 3) Re-bind cache server port to Virtual Server. For any modifications that need to be made to the cache-server, first unbind the cache server port from the Virtual Server, make the modifications and re-bind the cache-server port to the Virtual Server.	
Probability: Low	
Feature: TCS	**Function:** SNMP MIB based load balancing
Reported In Release: SI 12.2.00	**Service Request ID:** 267910

Defect ID: DEFECT000327031	**Technical Severity:** Medium
Summary: In TCS setup when ServerIron ADX receives packet matching an existing spoofed session and the Layer 3 state of the cache server is not ACTIVE then it sends out packet to the cache server instead of dropping it.	
Symptom: In TCS setup when ServerIron ADX receives packet matching an existing spoofed session and the Layer 3 state of the cache server is not ACTIVE then it sends out packet to the cache server instead of dropping it.	
Workaround: Clear MAC address of the cache server on both Active and Standby ServerIron ADXes.	
Probability: High	
Feature: TCS	**Function:** TCS L4
Reported In Release: SI 12.2.01	**Service Request ID:** 268269

Defect ID: DEFECT000327032	**Technical Severity:** Medium
Summary: ServerIron ADX does not drop the packets matching a spoofed session and received on a given port even though the destination mac address of the received packet is learnt on the incoming port.	
Symptom: ServerIron ADX does not drop the packets matching a spoofed session and received on a given port even though the destination mac address of the received packet is learnt on the incoming port.	
Probability: High	
Feature: TCS	**Function:** TCS L4
Reported In Release: SI 12.2.01	**Service Request ID:** 267608
Defect ID: DEFECT000306723	**Technical Severity:** Critical
Summary: ServerIron ADX application CPU may perform system reset when updating TCS statistics on an invalid port for which memory is not initialized.	
Symptom: ServerIron ADX application CPU performed system reset while adding "max-conn <value>" under cache-server configuration. As per analysis, system reset was not caused by this command.	
Probability: Low	
Feature: TCS	**Function:** TCS L4
Reported In Release: SI 12.1.00	**Service Request ID:** 255461

Defect ID: DEFECT000318375	**Technical Severity:** Critical
Summary: ServerIron ADX drops IPv6 Network Advertisements for pass-through traffic.	
Symptom: Network Advertisements for pass-through traffic between Host and Router is dropped by a ServerIron ADX. ICMPv6 echo requests passing through ServerIron ADX were dropped on the Application Processor (BP).	
Probability: High	
Feature: IPv6 Forwarding	**Function:** MP L3 Forwarding
Reported In Release: SI 12.2.00	**Service Request ID:** 259412

Defect ID: DEFECT000321277	**Technical Severity:** High
Summary: When TCS is configured with L7 switching, a ServerIron ADX sends connections to the internet instead of available cache-servers once the max-conn for a cache-server value is reached.	
Workaround: Remove CSW policy under cache-group.	
Probability: High	
Feature: L7 TCS	**Function:** SCALABILITY
Reported In Release: SI 12.1.00	**Service Request ID:** 261025

Defect ID: DEFECT000324516	**Technical Severity:** Medium
Summary: The command "summary" in debug filter mode may cause a ServerIron ADX to go into unresponsive state.	
Symptom: If the user enters the command "summary" in debug filter mode after capturing the packets ServerIron ADX may go into unresponsive state.	
Workaround: Use debug filter mode with very specific filters and with small buffer-size and packet size.	
Probability: Medium	
Feature: Debug filter	**Function:** Debug filter : Software
Reported In Release: SI 12.1.00	**Service Request ID:** 00266296

Closed with code in ServerIron ADX 12.2.1

Defect ID: DEFECT000296184	**Technical Severity:** High
Summary: FTP user data connection sessions are not synced with control session.	
Symptom: FTP user data connection sessions are not synced with control session.	
Feature: HA-Symmetric	**Function:** Fast Session Synchronization
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000298137	**Technical Severity:** Medium
Summary: After ServerIron ADX is reloaded, OSPF does not come up if MD-5 authentication is configured.	
Symptom: After ServerIron ADX is reloaded, OSPF does not come up if MD-5 authentication is configured.	
Workaround: Remove and add OSPF configuration under the interface. Do not configure MD5-Authentication	
Probability: High	
Feature: OSPF	**Function:** PROTOCOL
Reported In Release: SI 12.1.00	**Service Request ID:** 248278

Defect ID: DEFECT000300762	**Technical Severity:** Medium
Summary: The command "ip tcp syn-proxy-ack-validate-multiplier" does not work with value more than 2.	
Symptom: Customer configured "ip tcp syn-proxy-ack-validate-multiplier" command with value 32. This did not work.	
Workaround: Configure "ip tcp syn-proxy-ack-validate-multiplier" with a value less than or equal to 2.	
Feature: SYN-Proxy	**Function:** CLI
Reported In Release: SI 12.1.00	**Service Request ID:** 00246736

Defect ID: DEFECT000300876	**Technical Severity:** High
Summary: ServerIron ADX allows only one user to be logged into it at a given time via WEB GUI.	
Symptom: ServerIron ADX allows only one user to be logged into it at a given time via WEB GUI. Previous user will get disconnected before another user gets connected.	
Feature: Web Management	**Function:** L4-7 Pages
Reported In Release: SI 12.1.00	**Service Request ID:** 249328

Defect ID: DEFECT000300899	**Technical Severity:** Critical
Summary: With certain ServerIron ADX chassis MAC addresses, AXP CAM programming is not done correctly.	
Symptom: When customer enabled FTP port under server "cache-name" on the ServerIron ADX then the pass-through DNS traffic started failing as it started dropping the DNS response packets.	
Feature: AXP CAM	**Function:** CAM entry management
Reported In Release: SI 12.1.00	**Service Request ID:** 250054

Defect ID: DEFECT000301191	**Technical Severity:** High
Summary: ServerIron ADX does not use correct source-mac address when it uses source-ip address of the "VE interface" while sending out packet generated by itself.	
Symptom: ServerIron ADX does not use source-mac address of the "VE interface" when it uses source-ip address of the "VE interface" while sending out self-generated packets such as for Health check.	
Feature: L2 Forwarding	**Function:** MP L2 forwarding
Reported In Release: SI 12.1.00	**Service Request ID:** 250596

Defect ID: DEFECT000301273	**Technical Severity:** High
Summary: For IPv6 SLB, persist-hash fails resulting into a different server for the same client.	
Symptom: When persist-hash is configured under the vip port ,connections from the same IPv6 client are not sent to the same real server. Connections are sent out to different real servers .	
Workaround: Don't use persist-hash SLB with IPv6. Don't use any IP or network hash-based SLB with IPv6.	
Feature: IPV6 L4/7	**Function:** Ipv6 address maps
Reported In Release: SI 12.1.00	**Service Request ID:** 248665

Defect ID: DEFECT000301309	**Technical Severity:** Medium
Summary: maximum value of TCP connection in a real server is unsigned int16. Should be unsigned in32	
Symptom: The following log message will be seen when maximum value of TCP connection is reached:- May 4 16:44:06 <local4.notice> 10.10.10.10 SLB1, Server 100.100.100.100 named rs1 on port 25 has reached max-conn 65535 May 4 16:44:06 <local4.notice> 10.10.10.10 SLB1, Server 100.100.100.101 named rs2 on port 25 has reached max-conn 65535	
Feature: Conn Limit	**Function:** TCP Max Conn
Reported In Release: SI 12.1.00	**Service Request ID:** 250639

Defect ID: DEFECT000301531	**Technical Severity:** High
Summary: ServerIron ADX performs system reset when user tries to do SNMP GET query for snL4WebCacheGroupEntry	
Symptom: ServerIron ADX performs system reset when user tries to do SNMP GET query for snL4WebCacheGroupEntry.	
Probability: High	
Feature: SNMP Management	**Function:** Layer4-7 Mib
Reported In Release: SI 12.1.00	**Service Request ID:** 00251051

Defect ID: DEFECT000301965	**Technical Severity:** High
Summary: ServerIron ADX responds with TCP RESET for client connections to VIP when syn-proxy is configured along with global default TRL even though TRL is not applied to the interface.	
Symptom: Traffic to the Virtual IP fails	
Workaround: Reload the ServerIron after configuring default TRL.	
Probability: High	
Feature: Conn Limit	**Function:** TCP Conn Rate
Reported In Release: SI 12.1.00	**Service Request ID:** 251495

Defect ID: DEFECT000302202	**Technical Severity:** Medium
Summary: With TOS-marking and L3 DSR enabled, sessions may get piled up if the connection rate is high as the sessions are not deleted fast enough after receiving TCP FIN from the client.	
Symptom: With TOS-marking and L3 DSR enabled, sessions may get piled up if the connection rate is high due to half-closed connections as ServerIron ADX does not see reverse FIN in DSR mode.	
Feature: L4 SLB	**Function:** DSR
Reported In Release: SI 12.1.00	**Service Request ID:** 254934

Defect ID: DEFECT000302240	**Technical Severity:** Medium
Summary: If unconfigured policy is added to cache-group, error message is misleading.	
Symptom: User may see misleading error message, when an unconfigured policy is added to cache-group.	
Feature: L7 TCS	**Function:** CLI
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000302241	**Technical Severity:** Medium
Summary: In case of TCS+CSW configuration, CSW hash search url does not accept 0 as input, but converts 65536 to length 0.	
Symptom: In case of TCS+CSW configuration, CSW hash search url does not accept 0 as input, but converts 65536 to length 0.	
Feature: L7 TCS	**Function:** CLI
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000302270	**Technical Severity:** High
Summary: Content switching doesn't perform as expected when the CSW policy has search-url with offset 0 and length 1 in CSW+TCS configuration.	
Symptom: Content switching doesn't perform as expected when the CSW policy has search-url with offset 0 and length 1 in CSW+TCS configuration.	
Feature: L7 TCS	**Function:** CSW action
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000302534	**Technical Severity:** Medium
Summary: ServerIron ADX does not timeout BP-to-MP transactions while collecting information from BP when "save tech-support" command is executed and prints error messages when the same command is entered multiple times.	
Symptom: Customer could not execute "save tech-support" commands on ServerIron ADX one after another and it printed error messages as "Err: A print to file session is active, please try again later".	
Probability: Medium	
Feature: MP System	**Function:** save tech show short-tech
Reported In Release: SI 12.1.00	**Service Request ID:** 251649

Defect ID: DEFECT000303941	**Technical Severity:** Medium
Summary: A system reset is triggered when an ARP request packet with a sender mac different from the source mac in the ethernet header arrives on the management port	
Symptom: An ARP request packet with a sender mac different from the source mac in the ethernet header arriving on the management port caused a system reset.	
Feature: Management port	**Function:** Address configuration
Reported In Release: SI 12.1.00	**Service Request ID:** 255449

Defect ID: DEFECT000304179	**Technical Severity:** Critical
Summary: ServerIron does not free up SSL-slots whenever complete SSL health check for the non-Standard port such as 9443 fails.	
Symptom: ServerIron ADX stops performing complete SSL health checks for the non-standard ports over the period of time.	
Workaround: Disable complete ssl health checks on non standard ssl ports	
Probability: High	
Feature: Health checks	**Function:** L7 health checks
Reported In Release: SI 12.1.00	**Service Request ID:** 253145

Defect ID: DEFECT000304259	**Technical Severity:** Medium
Summary: ServerIron ADX may perform system reset when IPv6 VIP and IPv6 loopback interface are defined with the ip addresses in the same subnet.	
Symptom: ServerIron ADX may perform system reset when IPv6 VIP and IPv6 loopback interface are defined with the ip addresses in the same subnet.	
Workaround: Do not configure an IPv6 VIP and IPv6 loopback interface with the ip addresses in the same subnet.	
Feature: IPv6 Forwarding	**Function:** MP L3 Forwarding
Reported In Release: SI 12.1.00	**Service Request ID:** 254166

Defect ID: DEFECT000305271	**Technical Severity:** Medium
Summary: ServerIron ADX configured with SSL terminate and CSW does not perform redirection under certain circumstances.	
Symptom: CSW redirection with SSL terminate does not work. This problem is not seen with http. In the url debug output it looks like the SSL packet is getting corrupted.	
Probability: High	
Feature: L7 SLB Full Stack	**Function:** CSW action
Reported In Release: SI 12.1.00	**Service Request ID:** 00254516

Defect ID: DEFECT000305483	**Technical Severity:** Medium
Summary: Policy Based Routing does not work for DNS SLB traffic when source-nat is configured.	
Symptom: With Policy Based Routing configured for DNS VIP with source-nat, ServerIron ADX uses IP route instead of next-hop defined in PBR policy.	
Workaround: Remove source-nat if possible. Typically source-nat is used because of the one-armed topology so need to be careful while removing it. If it is the case, you may want to change the real server's gateway to be ServerIron	
Feature: Policy based routing	**Function:** Policy based routing : SLB
Reported In Release: SI 12.1.00	**Service Request ID:** 254366

Defect ID: DEFECT000306197	**Technical Severity:** Medium
Summary: CLI "aaa authentication web-server default local" always gets inserted into running configuration after reload	
Symptom: The CLI command "aaa authentication web-server default local" was automatically inserted into the running configuration after a power outage even with no trace of the command in the startup configuration.	
Feature: Web authentication	**Function:** Web Authentication
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000306272	**Technical Severity:** High
Summary: ServerIron ADX may perform a system reset when issuing a "show short-tech-support" command immediately after a command "save tech-support html <filename.html>"	
Symptom: ServerIron ADX performed a system reset when user issued a "show short-tech-support" command immediately after a command "save tech-support html <filename.html>"	
Workaround: Wait till you see DONE before issuing any additional commands after you issue "save tech html <filename..html>" command.	
Feature: Crash Dump	**Function:** MP Dump
Reported In Release: SI 12.1.00	**Service Request ID:** 255297

Defect ID: DEFECT000306619	**Technical Severity:** Medium
Summary: ServerIron ADX may perform system reset when it receives SNMP GET packet from the client which is configured to be denied with SNMP-ACL commands.	
Symptom: ServerIron ADX performed system reset when it received SNMP GET packet from the client which is configured to be denied with SNMP-ACL commands.	
Workaround: Remove the SNMP deny ACL “ro <acl-id>”; from the configured command snmp-server community public “ro <acl-id>”.	
Probability: Medium	
Feature: Crash Dump	**Function:** MP Dump
Reported In Release: SI 12.1.00	**Service Request ID:** 255575

Defect ID: DEFECT000306723	**Technical Severity:** Critical
Summary: ServerIron ADX application CPU may perform system reset when updating TCS statistics on an invalid port for which memory is not initialised	
Symptom: ServerIron ADX application CPU performed system reset while adding "max-conn <value>" under cache-server configuration. As per analysis, system reset was not caused by this command.	
Feature: TCS	**Function:** TCS L4
Reported In Release: SI 12.1.00	**Service Request ID:** 255461

Defect ID: DEFECT000306796	**Technical Severity:** Critical
Summary: Cookie switching does not work on SSL termination+CSW VIP when csw-rule match is based on "search" of text within the cookie header	
Symptom: ServerIron ADX did not recognize the Server ID when cookie switching is configured with csw-rule match based on "search" of text within the cookie header and with SSL termination. No issues were seen for the same VIP with port http and same CSW policy. Moreover the packet capture taken on the client for the SSL connection reveals that the client is actually sending the cookie with server ID but the ServerIron could not recognize it.	
Workaround: Define the csw-rule to match criteria as a "pattern" instead of as a "search".	
Probability: Medium	
Feature: L7 SLB Full Stack	**Function:** CSW action
Reported In Release: SI 12.1.00	**Service Request ID:** 00255672

Defect ID: DEFECT000306836	**Technical Severity:** Critical
Summary: ServerIron ADX MP CPU may perform system reset when user accidentally enters into special debug mode and performs invalid exit from mode while application CPU is booting up	
Symptom: Customer noticed older crashdumps for application CPU when executed the command "save tech-support". The timestamp was pointing to last system reboot.	
Workaround: Not to enter into debug mode.	
Feature: I2C Devices	**Function:** Debug
Reported In Release: SI 12.1.00	**Service Request ID:** 255693

Defect ID: DEFECT000306916	**Technical Severity:** High
Summary: Symmetric/sym-active HA: VIP failover takes 8 seconds during which VIP on both boxes shows as standby	
Symptom: Symmetric/sym-active HA: VIP failover takes 8 seconds during which VIP on both boxes shows as standby	
Workaround: Reduce sym-pdu-rate using the command server sym-pdu-rate	
Feature: HA-Symmetric	**Function:** Failover handling
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000306930	**Technical Severity:** Medium
Summary: The MP utilization is affected significantly when system-max vlan 4095 is configured	
Symptom: MP utilization is high around 50~99% compared to the traffic amount the MP receives. For example, 1,000 PPS targeted at the mgmt IP is enough to cause 99% MP utilization when system-max vlan 4095 is configured.	
Feature: VLAN	**Function:** VLAN flooding
Reported In Release: SI 12.1.00	**Service Request ID:** 253585

Defect ID: DEFECT000307186	**Technical Severity:** Medium
Summary: ServerIron ADX configured with Single Spanning Tree Protocol (SSTP) sends out BPDUs on untagged ports with VLAN ID tag as 4094 which happens to be a control VLAN used locally on the system for SSTP.	
Symptom: ServerIron ADX configured with Single Spanning Tree Protocol (SSTP) sent out BPDUs on untagged ports with VLAN ID tag as 4094 which happens to be a control VLAN used locally on the system for SSTP. This caused STP to not work properly.	
Feature: STP	**Function:** Single Spanning Tree
Reported In Release: SI 12.1.00	**Service Request ID:** 00256049

Defect ID: DEFECT000307187	**Technical Severity:** Medium
Summary: Executing "show ip nat translation" command on application CPU may cause it to perform a reset if there are many entries to be displayed.	
Symptom: Customer was having more than 2000 entries and when executed "show ip nat translation" command on application CPU it caused a system reset.	
Feature: IP NAT	**Function:** Dynamic NAT
Reported In Release: SI 12.1.00	**Service Request ID:** 00255311

Defect ID: DEFECT000307350	**Technical Severity:** Medium
Summary: When user enables “spanning-tree single” on ServerIron ADX configured with IP NAT then "ip nat inside" and "ip nat outside" commands get appended to all tagged physical interfaces of that VE.	
Symptom: When user enabled “spanning-tree single” on ServerIron ADX which was already configured with IP NAT, he noticed "ip nat inside" and "ip nat outside" under all physical interfaces which were part of VE enabled with IP NAT.	
Probability: Medium	
Feature: IP NAT	**Function:** Dynamic NAT
Reported In Release: SI 12.1.00	**Service Request ID:** 253563

Defect ID: DEFECT000307362	**Technical Severity:** Medium
Summary: ServerIron ADX Management CPU under certain circumstances and during bringing up application CPUs may cause memory corruption due to overwriting data. In some cases it may perform a system reset.	
Symptom: ServerIron ADX Management CPU performed system reset during bringing up application CPUs while user was logged in via Telnet session.	
Probability: Low	
Feature: MP System	**Function:** BP crash/bringup sequence
Reported In Release: SI 12.1.00	**Service Request ID:** 255963

Defect ID: DEFECT000307363	**Technical Severity:** Medium
Summary: Need to add diagnostic commands to identify the root cause of the Application CPU buffer loss issues.	
Symptom: ServerIron ADX restarted or reset application CPU when IPC communication between MP CPU and application CPU is broken due to buffer loss on a application CPU. The root cause of the buffer loss could not be determined as respective diagnostic commands are not available.	
Probability: Low	
Feature: Diagnostics	**Function:** ASM BP to BP dma diags
Reported In Release: SI 12.1.00	**Service Request ID:** 255963

Defect ID: DEFECT000307548	**Technical Severity:** Medium
Summary: Even though a SSL termination VIP port is down, the SI perfoms SSL handshake with clients, taking unnecesary BP CPU cycles.	
Symptom: Even though a SSL termination VIP port is down, the SI perfoms SSL handshake with clients, taking unnecesary BP CPU cycles.	
Probability: Medium	
Feature: SSL	**Function:** SSL protocol
Reported In Release: SI 12.1.00	**Service Request ID:** 252328

Defect ID: DEFECT000307653	**Technical Severity:** Medium
Summary: Critical IPC event such as when available HW-BUFFER on BP is less than 4K then a syslog message should be logged locally and sent to a syslog server	
Symptom: Customer ran out of BP buffers which caused BP to restart but there was no such error message logged before running out of buffers.	
Feature: IPC	**Function:** Debug
Reported In Release: SI 12.1.00	**Service Request ID:** 255963

Defect ID: DEFECT000307741	**Technical Severity:** Medium
Summary: ServerIron ADX print the following error message when user tries to define ssl-terminate for ldaps port : "Error : Can't config this PORT with ssl-terminate". SSL-termination works fine.	
Symptom: Customer was trying to define "ssl-terminate" for virtual port "ldaps" on ServerIron ADX and it threw the following error message : "Error : Can't config this PORT with ssl-terminate". SSL-termination works fine.	
Workaround: This is a display issue. You can ignore this safely.	
Feature: SSL	**Function:** SSL protocol
Reported In Release: SI 12.1.00	**Service Request ID:** 256206

Defect ID: DEFECT000307848	**Technical Severity:** Medium
Summary: ServerIron ADX application CPU may perform system reset when system has non-head fragmented packet in frag queue	
Symptom: Customer experienced a system reset on application CPU while processing fragmented traffic.	
Probability: Low	
Feature: IP Fragmentation	**Function:** CLI
Reported In Release: SI 12.1.00	**Service Request ID:** 256102

Defect ID: DEFECT000308008	**Technical Severity:** Medium
Summary: ServerIron ADX drops the SIP INVITE messages with URI length of more than 64 characters.	
Symptom: Certain outbound calls towards certain VOIP phones did not work.	
Probability: High	
Feature: SIP LB	**Function:** UDP processing
Reported In Release: SI 12.1.00	**Service Request ID:** 254739

Defect ID: DEFECT000308019	**Technical Severity:** Critical
Summary: ServerIron ADX configured with TCS for cache-bypass may perform system reset for application CPU when internal bypass-counter overflows.	
Symptom: ServerIron's application CPU was resetting with TCS configured along with the command "server cache-bypass".	
Workaround: Removing "server cache-bypass" command from the configuration will prevent system resets.	
Probability: Low	
Feature: TCS	**Function:** TCS L4
Reported In Release: SI 12.1.00	**Service Request ID:** 255194

Defect ID: DEFECT000308736	**Technical Severity:** Critical
Summary: Application CPU may perform system reset on ServerIron ADX configured with SIP-Stateful during deleting or aging SIP sessions.	
Symptom: Application CPU performed system reset when user tried to add configuration such as adding real server and its ports. But the issue also can be caused without config change due to session aging and accessing invalid session.	
Workaround: Configure SIP-switching instead of SIP-Stateful.	
Feature: SIP LB	**Function:** CLI
Reported In Release: SI 12.1.00	**Service Request ID:** 256744

Defect ID: DEFECT000308965	**Technical Severity:** Medium
Summary: ServerIron ADX forwards non-SYN packets with unknown DMAC to real servers instead of L2 switching even though 'use-session-for-vip-mac' is configured.	
Symptom: ServerIron ADX was forwarding non-SYN packets with unknown DMAC to real servers instead of L2 switching even though 'use-session-for-vip-mac' was configured. Once the DMAC was learnt, the 'server use-session-for-vip-mac' worked as expected.	
Workaround: The issue is seen only when ServerIron ADX does not have a corresponding MAC entry. This condition is seen intermittently.	
Probability: Low	
Feature: L4 SLB	**Function:** Session Management
Reported In Release: SI 12.1.00	**Service Request ID:** 249045

Defect ID: DEFECT000309278	**Technical Severity:** Medium
Summary: "save tech-support" can not be copied to TFTP server under certain circumstances and ServerIron ADX prints error message such as ".Flash Read Failed"	
Symptom: ServerIron-ADX#copy flash tftp 210.157.4.11 20100630-2.txt 20100630-2.txt copy err -1 Flash Read Failed Flash to TFTP Error - code 2	
Workaround: 1) Use an external usb instead of tftp. 2) Use faster tftp server software and have TFTP server as close to ADX as possible to eliminate packet drops caused due to network congestion.	
Feature: MP System	**Function:** Image updates
Reported In Release: SI 12.1.00	**Service Request ID:** 255957

Defect ID: DEFECT000309290	**Technical Severity:** High
Summary: Removing a dynamic NAT mapping disables a virtual server when the ip addresses for the virtual server and the dynamic NAT pool are same.	
Symptom: If a customer removes a static or dynamic NAT mapping where the inside global and inside local addresses overlap an SLB mapping between virtual and real server, the virtual server stops responding to client traffic.	
Workaround: Temporarily remove the virtual server before removing the NAT mapping.	
Probability: High	
Feature: IP NAT	**Function:** Dynamic NAT
Reported In Release: SI 12.2.00	**Service Request ID:** 255221

Defect ID: DEFECT000309472	**Technical Severity:** High
Summary: ServerIron ADX may lose TCB buffers during bringup of real server ports when it alternately tries to bringup secure and http ports.	
Symptom: Customer observed that ServerIron ADX was not sending out health check packets to any cofnigured real or remote servers. "show ip tcp connection" command output indicated all TCP buffers being used even though those connections were stale.	
Workaround: Configure "no server no-fast-bringup" command globally or "no no-fast-bringup" under SSL port profile and then write to memory. Reload is required to recover from this situation.	
Probability: Medium	
Feature: Health checks	**Function:** L7 health checks
Reported In Release: SI 12.1.00	**Service Request ID:** 256719

Defect ID: DEFECT000309693	**Technical Severity:** Medium
Summary: TCS is perfomed even though 'no cache-group' is configured on the trunk if a packet is received on the secondary port	
Symptom: TCS is perfomed even though 'no cache-group' is configured on the trunk if a packet is received on the secondary port. Due to the above reason, a TCP connection breaks intermittenly because packets belonging to the same socket can be forwarded to different cache servers.	
Feature: TCS	**Function:** TCS L4
Reported In Release: SI 12.1.00	**Service Request ID:** 242959

Defect ID: DEFECT000309699	**Technical Severity:** Medium
Summary: MP resets on ADX when U3 enabled USB drive is inserted and accessed	
Symptom: MP resets when user inserts a Kingston DataTraveler and U3 Smart software and issue any sort of flash command that will access the USB drive such as “show flash”.	
Feature: OS	**Function:** Code flash file system
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000310169	**Technical Severity:** Medium
Summary: SSH session hangs when 'show server source-nat-ip' is executed using TACACS+ authorization.	
Symptom: When you have Cisco TACACS configured, If you run the "show server source-nat-ip" command with out any IP address, your sessions hangs up. You can not control C or cancel out of the session. You have to login via another session and do a 'kill ssh <session#>' to end the old session. This issue is not seen with Telnet or Console	
Workaround: 1.) Use Telnet or Console 2.) Use the command with a source-ip. E.g: show server source-nat-ip 10.253.179.1	
Probability: Medium	
Feature: SSH	**Function:** CLI
Reported In Release: SI 12.1.00	**Service Request ID:** 256909

Defect ID: DEFECT000310978	**Technical Severity:** High
Summary: Linecards will get stuck in a tuning loop upon bootup with a fully loaded 10U....	
Symptom: Linecards will get stuck in a tuning loop upon bootup with a fully loaded 10U....	
Feature: MP Boot Sequence	**Function:** Bringup linecard modules
Reported In Release: SI 12.2.00	

Defect ID: DEFECT000311845	**Technical Severity:** Critical
Summary: ADX may reset when performing certain web management access.	
Symptom: ADX may reset when performing certain web management access.	
Feature: Web Management	**Function:** HTTP Engine
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000312727	**Technical Severity:** Critical
Summary: Application Processors may reset when they receive a packet routed to the null0 interface.	
Symptom: Application Processors may reset when they receive a packet routed to the null0 interface.	
Workaround: Remove any routes pointing at null0.	
Probability: High	
Feature: IP Forwarding	**Function:** BP L3 Forwarding
Reported In Release: SI 12.1.00	**Service Request ID:** 258858

Defect ID: DEFECT000313267	**Technical Severity:** High
Summary: ServerIron ADX configured for IP NAT and SLB where VIP is same as NAT IP, SLB traffic fails once after single IP NAT connection initiated from the real server.	
Symptom: SLB VIP was not working. SLB VIP and NAT IP are the same. There were already IP NAT sessions on the system.	
Feature: IP NAT	**Function:** Dynamic NAT
Reported In Release: SI 12.2.00	**Service Request ID:** 257134

Defect ID: DEFECT000313352	**Technical Severity:** High
Summary: TCP SLB connections are not maintained through hot standby failover when ports are translated.	
Symptom: TCP SLB connections are not maintained through hot standby failover when ports are translated.	
Workaround: Close the connection and open a new one.	
Probability: High	
Feature: HA-Hotstandby	**Function:** Failover handling
Reported In Release: SI 12.1.00	**Service Request ID:** 258988

Defect ID: DEFECT000313496	**Technical Severity:** Medium
Summary: ServerIron does not redirect TCS traffic for non-standard ports if more than 32 non-standard ports are configured under the cache server.	
Symptom: Users may experience connectivity issues to their application since the application only allows the proxies to connect to them and some of the connections for non-standard ports were being sent to the internet directly by the ServerIron.	
Workaround: Customer will need to configure the non-standard ports to 32 for each cache server until the defect is fixed.	
Probability: High	
Feature: TCS	**Function:** TCS L4
Reported In Release: SI 12.1.00	**Service Request ID:** 00258411

Defect ID: DEFECT000313624	**Technical Severity:** Medium
Summary: Undefined real server binding removed from a VIP may cause ServerIron ADX to reset	
Symptom: When an undefined real server binding removed from a VIP, Management CPU on ADX resets.	
Probability: Medium	
Feature: L4 SLB	**Function:** Sever selection
Reported In Release: SI 12.1.00	**Service Request ID:** 00257961

Defect ID: DEFECT000313676	**Technical Severity:** Medium
Summary: Removing a SNTP server config which is not reachable causes ADX to reset	
Symptom: When a SNTP server which is not reachable anymore is removed from the configuration, Management CPU may reset. For this issue, the SNTP server should have been accessible before and should not be accessible when the config is removed	
Workaround: - Disable the interface that is used to reach the SNTP server and then remove SNTP configuration. - Add another SNTP server that is accessible before removing the server that is unreachable	
Probability: Medium	
Feature: SNTP	**Function:** CLI
Reported In Release: SI 12.1.00	**Service Request ID:** 00258882

Defect ID: DEFECT000314160	**Technical Severity:** Medium
Summary: ADX:- Static route pointing to loopback address disappear after reload	
Symptom: When a static route whose next hop is loopback address is configured, the route will disappear after reload.	
Workaround: "clear ip route" will restore the route.	
Feature: OSPF	**Function:** CLI
Reported In Release: SI 12.1.00	**Service Request ID:** 00259150

Defect ID: DEFECT000314425	**Technical Severity:** High
Summary: ADX 64 bit counters do not give the correct information once the value of the counter is greater than 32 bit value	
Symptom: MIB "snL4VirtualServerStatisticReceiveBytes" value got decreased value from previous value after reaching a particular value	
Workaround: no work-around	
Probability: Medium	
Feature: Packet Processor	**Function:** Packet processing
Reported In Release: SI 12.1.00	**Service Request ID:** 00259393

Defect ID: DEFECT000314709	**Technical Severity:** High
Summary: url debug doesn't work when used with Client-IP	
Symptom: No output is seen after enabling url debug with cllent-ip specified. The connectio n works but no debug output is received.	
Workaround: Use 'url debug' without specifying client-ip CAUTION: This should be only done if the client requests are less than 10. If it is used when there are many connections, it could potentially hog down the box due to amount of debug output generated.	
Probability: High	
Feature: L7 SLB Full Stack	**Function:** Debug
Reported In Release: SI 12.1.00	**Service Request ID:** 259561

Defect ID: DEFECT000316045	**Technical Severity:** Medium
Summary: Loopback interface cannot be ping'd after the ADX is reloaded (12.2.00)	
Symptom: Loopback interface cannot be ping'd after the ADX is reloaded.	
Feature: Neighbor Discovery	**Function:** Neighbor learning
Reported In Release: SI 12.2.00	**Service Request ID:** 00260401

Defect ID: DEFECT000316438	**Technical Severity:** Medium
Summary: A static route to the null0 interface that is redistributed into OSPF disappears from the OSPF database after reload.	
Symptom: A static route to the null0 interface that is redistributed into OSPF disappears from the OSPF database after reload.	
Probability: High	
Feature: OSPF	**Function:** PROTOCOL
Reported In Release: SI 12.1.00	**Service Request ID:** 260674

Defect ID: DEFECT000318920	**Technical Severity:** Medium
Summary: An NXP part change in the latest revision switch fabric hardware may cause I2C to fail, and may result in system problem.	
Symptom: A system may boot-up but not forward any packets if it is running a revision of the Switch Fabric which is shipped after 20th September, 2010.	
Workaround: Fix checked into 12.2.1, 12.1f branches - automatically would get into 12.3	
Feature: Diagnostics	**Function:** MP Memory Diags
Reported In Release: SI 12.1.00	

Open Defects in the ServerIron ADX 12.2.1

This section lists defects with Critical, High, and Medium Technical Severity open in version 12.2.1 for ServerIron ADX application switches. While these defects are still formally "open," they are unlikely to impede Brocade customers in their deployment of version 12.2.1 and have been deferred to a later release.

None of these defects have the requisite combination of probability and severity to cause significant concern to Brocade customers.

Defect ID: DEFECT000295270	**Technical Severity:** High
Summary: Longest match first criteria fails for response rewrite when server sends response with chunk, and packets split at longer matched pattern.	
Symptom: Longest match first criteria fails for response rewrite when server sends response with chunk, and packets split at longer matched pattern.	
Feature: Response rewrite	**Function:** response body rewrite
Reported In Release: SI 12.2.00	

Defect ID: DEFECT000301891	**Technical Severity:** High
Summary: Under certain conditions, Application processor may reset if "apply port-range" command is issued while virtual/real ports are in closing state.	
Symptom: Under certain conditions, Application processor may reset if "apply port-range" command is issued while virtual/real ports are in closing state.	
Workaround: The following steps can be used as workaround. --> Disable virtual server that is configured with the port-range that is modified. This will not allow any new connection to this virtual server. --> Wait till all the existing sessions are aged out or clear the sessions of bound real servers. --> Then issue the "apply port-range" command.	
Feature: L4 SLB	**Function:** Port Range
Reported In Release: SI 12.2.00	

Defect ID: DEFECT000301941	**Technical Severity:** High
Summary: Some AXP counters pertaining to Syn Proxy feature do not increment correctly. Related counters in "show server tcp-attack" do not increment as well.	
Symptom: The output of "show server synproxy" and "show server tcp-attack" displays some counters related to the number of SYN packets received by AXP in the ServerIron. These counters do not increment properly. However, functionality is not affected and traffic is successfully processed by AXP and passed on to BP.	
Feature: SYN-Proxy	**Function:** CLI
Reported In Release: SI 12.2.00	

Defect ID: DEFECT000312261	**Technical Severity:** High
Summary: With CSW and Static Weighted Round Robin, traffic is load balanced to only one server when layer 7 criteria is not met.	
Symptom: With CSW and Static Weighted Round Robin, traffic is load balanced to only one server when layer 7 criteria is not met.	
Feature: L4 Server Selection	**Function:** Static Weighted Round Robin
Reported In Release: SI12.2.1	

Defect ID: DEFECT000315700	**Technical Severity:** High
Summary: L7 content switching (CSW) does not work when ServerIron is configured for TCS and the cache-group number configured is greater than 4	
Symptom: L7 content switching (CSW) does not work when ServerIron is configured for TCS and the cache-group number configured is greater than 4.	
Workaround: Configure cache-group numbers from 1 through 4 only, when configuring L7 content switching with TCS.	
Feature: L7 TCS	**Function:** CSW action
Reported In Release: SI12.2.1	

Defect ID: DEFECT000316126	**Technical Severity:** High
Summary: Cannot access (telnet/http) ServerIron using its IPv6 management address through syn-proxy enabled interface.	
Symptom: Cannot access (telnet/http) ServerIron using its IPv6 management address through syn-proxy enabled interface . ServerIron's management processor is receiving the SYN packet, but not responding with SYN-ACK, so it is causing access failure.	
Feature: SYN-Proxy	**Function:** Syn-Cookie with Opt SLB
Reported In Release: SI12.2.1	

Defect ID: DEFECT000317204	**Technical Severity:** High
Summary: FTP doesn't work after a failover in an Active-Active IP-NAT configuration if the NAT-Pool has more than one IP address.	
Symptom: Since the NAT helper session is not synched to the peer ServerIron, FTP control and data connections are using different NAT-Pool IP addresses, so it is causing failure of the data connection.	
Workaround: Reestablish FTP connection.	
Feature: IP NAT	**Function:** Dynamic NAT
Reported In Release: SI12.2.1	

Defect ID: DEFECT000311930	**Technical Severity:** High
Summary: Spoofing doesn't work for TCP traffic in Syn-Proxy configuration.	
Symptom: ServerIron sends out SYN-ACK on the same interface on which it received SYN, but the subsequent reverse traffic takes static route or PBR (if configured) instead of spoofing path.	
Feature: Policy based routing	**Function:** Policy based routing : SLB
Reported In Release: SI12.2.1	

Defect ID: DEFECT000294399	**Technical Severity:** Medium
Summary: HTTP status codes when configured under the port policy in certain ways do not get configured	
Symptom: HTTP status codes when configured under the port policy in certain ways do not get configured	
Feature: L4 SLB	**Function:** SCALABILITY
Service Request ID: 228094	
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000294828	**Technical Severity:** Medium
Summary: While doing SCP of a file which is not existing on machine to SI , SSH session might get hung	
Symptom: While doing SCP of a file which is not existing on machine to SI , SSH session might get hung	
Feature: SSL Key/Cert Management	**Function:** Scp key/cert files
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000295230	**Technical Severity:** Medium
Summary: show server virtual command does not display the correct state of vip port when minimum-healthy-real-server is configured	
Symptom: show server virtual command does not display the correct state of vip port when minimum-healthy-real-server is configured	
Feature: Health checks	**Function:** L2 health checks
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000295420	**Technical Severity:** Medium
Summary: IPv6 DSR healthcheks are not happening for the loopback address, ADX is sending syn to the physical address of real server	
Symptom: In IPv6 DSR config healthcheks are not happening for the loopback address, SI is sending syn to the physical address	
Feature: IPv6 mgmt stack	**Function:** Stack reachability
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000295618	**Technical Severity:** Medium
Summary: IPv6 ACL logging does not log anything when a Deny clause is hit.	
Symptom: Log action doesn't work when traffic hits IPv6 ACL deny rules. No problem with IPv4 ACL deny rules.	
Feature: ACL	**Function:** IPv6 ACL
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000295868	**Technical Severity:** Medium
Summary: DNS health check doesn't work properly if a dns profile is defined with "udp l4-check-only" and server no-fast-bringup	
Symptom: DNS health check starts failing	
Feature: Health checks	**Function:** L2 health checks
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000296022	**Technical Severity:** Medium
Summary: ADX is in undefined config mode when trying to switch to interface level config mode from trunk config mode	
Symptom: Users gets in un-defined config mode when she tries to switch from trunk-config-mode to multi-interface-config-mode. User can issue "exit" to get out of this mode.	
Feature: SYN-Proxy	**Function:** Software SYN-Cookie
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000296096	**Technical Severity:** Medium
Summary: On hot standby HA set-up, copy image from tftp to fl followed by "sh flash" causes HA failover	
Symptom: On hot standby HA set-up, copy image from tftp to flash followed by issuing "sh flash" causes HA failover.	
Workaround: User has to wait for 40-50 seconds before issuing "show flash" command after the completion of image copy.	
Feature: HA-Hotstandby	**Function:** Failover handling
Reported In Release: SI 12.2.00	

Defect ID: DEFECT000296195	**Technical Severity:** Medium
Summary: TCS+CSW: TCS sessions are not being synched to peer with server active-active port configured	
Symptom: TCS sessions are not being synched to peer in active-active CSW+TCS configuration. In case of L4 TCS (no CSW), configuring active-active port will enable session synchronization. In case of CSW+TCS configuration, users have to configure port profile for TCS ports and then enable "session-sync" for each port.	
Workaround: In case of CSW+TCS configuration, users have to configure port profile for TCS ports and then enable "session-sync" for each port.	
Feature: TCS	**Function:** TCS + URL switching
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000297629	**Technical Severity:** Medium
Summary: IPv4 source-nat-ip is not pingable from real server, but server load balancing using this source-nat-ip is not affected	
Symptom: IPv4 source-nat-ip is not pingable from real server, but server load balancing using this source-nat-ip is not affected	
Feature: Source NAT	**Function:** Source NAT CAM entries
Reported In Release: SI 12.2.00	

Defect ID: DEFECT000301258	**Technical Severity:** Medium
Summary: Trunk level configuration is not saved upon hot swap of a line-card module.	
Symptom: Trunk level configuration is not saved upon hot swap of a line-card module. For example, when one port of a trunk is disabled and then the line-card is hot swapped, the disabled trunk port will become enabled upon line-card bring-up.	
Workaround: User has to reconfigure trunk level configuration after line-card is up. Other workaround is to reload ServerIron-ADX.	
Feature: Trunk	**Function:** Trunk Deploy
Reported In Release: SI 12.2.00	

Defect ID: DEFECT000301987	**Technical Severity:** Medium
Summary: When the alias-port is bound first without binding the actual port of a real server to a virtual server port, or when using an invalid port alias configuration, the port-holddown feature is activated even without the port-holddown configuration.	
Symptom: When the alias-port is bound first without binding the actual port of a real server to a virtual server port, or when using an invalid port alias configuration, the port-holddown feature is activated even without the port-holddown configuration	
Feature: SLB	**Function:** Server holddown timer
Reported In Release: SI 12.2.00	

Defect ID: DEFECT000302516	**Technical Severity:** Medium
Summary: Deletion of a real/remote server with a host-range will not fully delete the host-range	
Symptom: If a real/remote server having the host-range command is deleted from the configuration, server hosts that fall under that host-range are not deleted internally. This will prevent the user from configuring real/remote servers with IP addresses belonging to that host-range.	
Workaround: The workaround for this issue is to first delete the host-range feature from the real/remote server and then delete the real/remote server afterwards.	
Feature: L4 SLB	**Function:** Host Range
Reported In Release: SI 12.2.00	

Defect ID: DEFECT000303104	**Technical Severity:** Medium
Summary: Layer 7 Health Check response in very small fragments causes server port's health check to get stuck in Testing state	
Symptom: 1. Problematic real servers are sending very small (2 - 20 bytes) responses to L7 requests from SI. 2. SI stops sending L4 and L7 keepalives once it receives a very small response from the server. 3. If the real server is configured for "l4-check-only" before keepalives are enabled, no issues are seen. L4 keepalives work correctly in such case. 4. If the real server's keepalives are changed from L7 to L4-check-only AFTER the problem is hit, the problem remains.	
Workaround: If server fast bringup is on, the problem is not observed. This is because, keepalive handles these small packets correctly. it is only bringup that has the problem.	
Feature: Health checks	**Function:** L7 health checks
Service Request ID: 246820	
Reported In Release: SI 12.1.00	**Probability:** Low

Defect ID: DEFECT000308491	**Technical Severity:** Medium
Summary: CLI allows to configure both OSPFv3 and IPv6-dont-advertise on an interface	
Symptom: CLI allows to configure both OSPFv3 and IPv6-dont-advertise on an interface. This combination is not allowed for IPv4 so IPv6 RHI also should refuse this config.	
Feature: Route health injection	**Function:** OSPFv3
Reported In Release: SI12.2.1	

Defect ID: DEFECT000314141	**Technical Severity:** Medium
Summary: The current-attack-rate counter in the output of the command "show server tcp-attack" is not updated in real-time	
Symptom: The command "show server tcp-attack" is used to check the current counters on client and server side pertaining to the SynProxy feature. The "current attack rate" counter in this output is not updated in real time and there is a 20 seconds delay between what is seen by the hardware, and what is reported by the counter.	
Feature: SYN-Proxy	**Function:** CLI
Reported In Release: SI12.2.1	

Defect ID: DEFECT000316088	**Technical Severity:** Medium
Summary: Unconfiguring IPv6 management address from ADX running switch code does not remove the reference to this address on application processors.	
Symptom: Since the reference to removed IPv6 management address is not removed on application processors, it may cause problems if the same address is used for some other host in the network.	
Workaround: A reload is required to flush the unconfigured ipv6 address entry on application processors.	
Feature: IPv6 mgmt stack	**Function:** Auto Address Configuration
Reported In Release: SI12.2.1	

Defect ID: DEFECT000317525	**Technical Severity:** Medium
Summary: Active FTP data session fails even though the traffic matches a PBR rule if a default gateway is not available.	
Symptom: Active FTP data session fails even though the traffic matches a PBR rule if a default gateway is not available.	
Feature: Policy based routing	**Function:** Policy based routing : SLB
Service Request ID: 255665	
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000304436	**Technical Severity:** Medium
Summary: In an ADX configured with IP NAT, Traffic routed through ADX is IP NAT'ed even when the outbound interface is not defined with "ip nat outside".	
Symptom: When IP NAT is configured on ADX and traffic matching the source IP in an ACL applied to IP NAT needs to be routed through the ADX but the outbound interface does not have "ip nat outside" defined, ADX still performs IP NAT on such traffic.	
Workaround: Define IP NAT ACL with specific source and destination so that traffic from a source IP matching the ACL associated with IP NAT, does not get NAT'ed when it needs to be routed out of an interface not defined with "ip nat outside".	
Feature: IP NAT	**Function:** Dynamic NAT
Service Request ID: 00247169	
Reported In Release: SI 12.1.00	**Probability:** High

Defect ID: DEFECT000306775	**Technical Severity:** Medium
Summary: ADX web management page is displayed when clients access http service of SLB VIP IP's if the ASM module is removed and a reload is done.	
Symptom: If the ADX BP's are down and the serverIron is reloaded, the cam tables are reprogrammed without the BP's, this causes all VIP traffic to go to the MP. In the case of the ServerIron ADX, the web management page will be displayed when clients access http service of SLB VIP IPs. ADX ServerIron is supposed to terminate the connections in this case.	
Feature: L4 SLB	**Function:** TCP Control packet handling
Reported In Release: SI 12.1.00	

Defect ID: DEFECT000312290	**Technical Severity:** Medium
Summary: Source-nat-ip configured on a router build is not pingable.	
Symptom: Source-nat-ip configured on a router build is not pingable. No problem is seen with source-nat functionality.	
Feature: Source NAT	**Function:** Source IP selection
Reported In Release: SI12.2.1	

Defect ID: DEFECT000313449	**Technical Severity:** Medium
Summary: SNMP MIB snChasPwrSupplyTable may not return the correct values	
Symptom: SNMP-Get on MIB snChasPwrSupplyTable will return invalid values.	
Feature: SNMP Management	**Function:** Layer4-7 Mib
Reported In Release: SI12.2.1	

Defect ID: DEFECT000314759	**Technical Severity:** Medium
Summary: Certain configurations are not copied when a real server is cloned.	
Symptom: The config option "l7-bringup-interval" is available and can be configured in real-server context. However, when the real server (T1) is cloned, the new server (T5) does not get this configuration. It's the same with the config "l4-bringup-interval"	
Feature: L7 SLB Pseudo Stack	**Function:** CLI
Reported In Release: SI12.2.1	

Defect ID: DEFECT000315656	**Technical Severity:** Medium
Summary: On an active-active FWLB HA set-up with SLB configured on both boxes, ping destined to the VIP from the ServerIron that is non-owner of the VIP does not work.	
Symptom: On an active-active FWLB HA set-up with SLB configured on both boxes, ping destined to the VIP from the ServerIron that is non-owner of the VIP does not work. No problem is seen with SLB+FWLB functionality.	
Feature: FWLB	**Function:** FWLB + External SLB
Reported In Release: SI12.2.1	

Defect ID: DEFECT000317079	**Technical Severity:** Medium
Summary: With multiple users logged into ServerIron web management, show web-connections on CLI displays information for the most recent web connection only.	
Symptom: With multiple users logged into ServerIron web management, show web-connections on CLI displays information for the most recent web connection only.	
Workaround: Show log shows the information for all web connections that are opened. Use show log instead of show web-connections.	
Feature: Web Management	**Function:** CLI
Reported In Release: SI12.2.1	

Defect ID: DEFECT000311215	**Technical Severity:** Medium
Summary: FTP traffic fails if spoofing is enabled for port ftp.	
Symptom: FTP helper sessions are not created if spoofing is enabled, so FTP data traffic is not translated in both active and passive FTP cases. It is causing traffic failure.	
Feature: Session Management	**Function:** Session creation
Reported In Release: SI12.2.1	

Defect ID: DEFECT000311443	**Technical Severity:** Medium
Summary: Spoofing doesn't work for UDP DNS traffic. No problem is seen with TCP DNS traffic.	
Symptom: Reverse UDP DNS traffic is taking static route path instead of spoofing path.	
Feature: DNS	**Function:** PROTOCOL
Reported In Release: SI12.2.1	

Defect ID: DEFECT000312890	**Technical Severity:** Medium
Summary: On a symmetric HA set-up, VIPs failover after a delay of 8 seconds when server delay-symmetric is configured	
Symptom: On a symmetric HA set-up, VIPs failover after a delay of 8 seconds when server delay-symmetric is configured. The 8 second delay is not seen with no delay symmetric configured.	
Feature: HA-Symmetric	**Function:** Failover handling
Reported In Release: SI12.2.1	